

01.10.2004

日 本 国 特 許 庁
JAPAN PATENT OFFICE

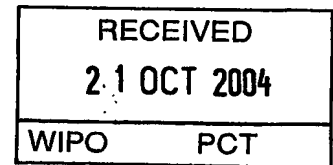
別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: 2 0 0 3 年 1 0 月 3 1 日

出 願 番 号
Application Number: 特 願 2 0 0 3 - 3 7 3 0 9 7
[ST. 10/C]: [J P 2 0 0 3 - 3 7 3 0 9 7]

出 願 人
Applicant(s): パイオニア株式会社

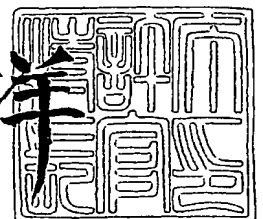


PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH
RULE 17.1(a) OR (b)

2 0 0 4 年 7 月 2 日

特許庁長官
Commissioner,
Japan Patent Office

小 川 洋



【書類名】 特許願
【整理番号】 58P0440
【あて先】 特許庁長官 殿
【国際特許分類】 H04L 9/06
G09C 1/00 610
【発明者】
【住所又は居所】 埼玉県所沢市花園 4 丁目 2 6 1 0 番地 パイオニア株式会社 所
沢工場内
【氏名】 多田 謙一郎
【特許出願人】
【識別番号】 000005016
【氏名又は名称】 パイオニア株式会社
【代理人】
【識別番号】 100083839
【弁理士】
【氏名又は名称】 石川 泰男
【電話番号】 03-5443-8461
【手数料の表示】
【予納台帳番号】 007191
【納付金額】 21,000円
【提出物件の目録】
【物件名】 特許請求の範囲 1
【物件名】 明細書 1
【物件名】 図面 1
【物件名】 要約書 1
【包括委任状番号】 9102133

【書類名】 特許請求の範囲**【請求項 1】**

少なくとも一の画像情報単位により構成される記録情報を、当該画像情報単位と異なる暗号化単位の境界において暗号鍵を変更しつつ暗号化して得られた暗号化情報が記録されている暗号化情報記録領域と、

前記暗号化情報における前記画像情報単位に含まれる静止画像情報の解読に複数の暗号鍵が必要か否かを示す鍵変更情報が記録されている鍵変更情報記録領域と、

を備えることを特徴とする情報記録媒体。

【請求項 2】

請求項 1 に記載の情報記録媒体において、

前記鍵変更情報記録領域は、前記画像単位毎に設けられていることを特徴とする情報記録媒体。

【請求項 3】

請求項 1 または 2 に記載の情報記録媒体において、

前記静止画像情報は、フレーム内符号化画像情報であることを特徴とする情報記録媒体。

【請求項 4】

請求項 1 乃至 3 のいずれか一項に記載の情報記録媒体において、

前記画像情報単位は、少なくとも一の前記フレーム内符号化画像情報を含む符号化画像情報群により構成されていることを特徴とする情報記録媒体。

【請求項 5】

請求項 1 乃至 4 のいずれか一項に記載の情報記録媒体において、

前記画像情報単位は、MPEG (Moving Picture Experts Group) - 2 TS (Transport Stream) のシーケンスヘッダと、前記シーケンスヘッダに後続して送信される GOP (Group Of Picture) データにより構成されていることを特徴とする情報記録媒体。

【請求項 6】

少なくとも一の画像情報単位により構成される記録情報を当該画像情報単位とは異なる暗号化単位の境界において暗号鍵を変更しつつ暗号化して得られた暗号化情報を生成する第 1 生成手段と、

前記暗号化情報における前記画像情報単位に含まれる静止画像情報の解読に複数の暗号鍵が必要か否かを示す鍵変更情報を記録する第 2 生成手段と、

を備えることを特徴とする情報記録装置。

【請求項 7】

請求項 6 に記載の情報記録装置において、

前記鍵変更情報記録領域は、前記画像単位毎に設けられていることを特徴とする情報記録装置。

【請求項 8】

請求項 6 または 7 に記載の情報記録装置において、

前記静止画像情報は、フレーム内符号化画像情報であることを特徴とする情報記録装置。

【請求項 9】

請求項 6 乃至 8 のいずれか一項に記載の情報記録装置において、

前記画像情報単位は、少なくとも一の前記フレーム内符号化画像情報を含む符号化画像情報群により構成されていることを特徴とする情報記録装置。

【請求項 10】

請求項 6 乃至 9 のいずれか一項に記載の情報記録装置において、

前記画像情報単位は、MPEG (Moving Picture Experts Group) - 2 TS (Transport Stream) のシーケンスヘッダと、前記シーケンスヘッダに後続して送信される GOP (Group Of Picture) データにより構成されていることを特徴とする情報記録装置。

【請求項 11】

少なくとも一の画像情報単位により構成される記録情報を、当該画像情報単位とは異なる暗号化単位の境界において暗号鍵を変更しつつ暗号化して得られた暗号化情報が記録されている暗号化情報記録領域と、前記暗号化情報における前記画像情報単位に含まれる静止画像情報の解読に複数の暗号鍵が必要か否かを示す鍵変更情報が記録される鍵変更情報記録領域と、が記録されている情報記録媒体から前記記録情報を再生する情報再生装置であって、

前記情報記録媒体から前記暗号化情報を検出する暗号化情報検出手段と、
前記情報記録媒体から前記鍵変更情報を検出する鍵変更情報検出手段と、
検出された前記鍵変更情報に基づいて前記暗号化情報を解読する解読手段と、
解読した前記暗号化情報を再生する再生手段と、
を備えることを特徴とする情報再生装置。

【請求項 12】

請求項 11 に記載の情報再生装置において、
前記鍵変更情報記録領域は、前記画像単位毎に設けられていることを特徴とする情報再生装置。

【請求項 13】

請求項 11 または 12 に記載の情報再生装置において、
前記静止画像情報は、フレーム内符号化画像情報であることを特徴とする情報再生装置。

【請求項 14】

請求項 11 乃至 13 のいずれか一項に記載の情報再生装置において、
前記画像情報単位は、少なくとも一の前記フレーム内符号化画像情報を含む符号化画像情報群により構成されていることを特徴とする情報再生装置。

【請求項 15】

請求項 11 乃至 14 のいずれか一項に記載の情報再生装置において、
前記画像情報単位は、MPEG (Moving Picture Experts Group) - 2 TS (Transport Stream) のシーケンスヘッダと、前記シーケンスヘッダに後続して送信される GOP (Group Of Picture) データにより構成されていることを特徴とする情報再生装置。

【請求項 16】

請求項 11 乃至 15 のいずれか一項に記載の情報再生装置において、
前記解読手段は、検出された前記鍵変更情報が、暗号化された一の前記静止画像情報を解読する処理において二以上の前記暗号鍵が必要であることを示す場合は、当該静止画像情報の解読に必要な暗号鍵を検索する検索手段を備えることを特徴とする情報再生装置。

【請求項 17】

少なくとも一の画像情報単位により構成される記録情報を当該画像情報単位とは異なる暗号化単位の境界において暗号鍵を変更した暗号化情報を生成する第 1 生成工程と、
前記暗号化情報における前記画像情報単位に含まれる静止画像情報の解読に複数の暗号鍵が必要か否かを示す鍵変更情報を記録する第 2 生成工程と、
を備えることを特徴とする情報記録方法。

【請求項 18】

少なくとも一の画像情報単位により構成される記録情報を、当該画像情報単位とは異なる暗号化単位の境界において暗号鍵を変更しつつ暗号化して得られた暗号化情報が記録されている暗号化情報記録領域と、前記暗号化情報における前記画像情報単位に含まれる静止画像情報の解読に複数の暗号鍵が必要か否かを示す鍵変更情報が記録される鍵変更情報記録領域と、が記録されている情報記録媒体から前記記録情報を再生する情報再生方法であって、

前記情報記録媒体から前記暗号化情報を検出する暗号化情報検出工程と、
前記情報記録媒体から前記鍵変更情報を検出する鍵変更情報検出工程と、
検出された前記鍵変更情報に基づいて前記暗号化情報を解読する解読工程と、
解読した前記暗号化情報を再生する再生工程と、

を備えることを特徴とする情報再生方法。

【請求項 19】

少なくとも一の画像情報単位により構成される記録情報を情報記録媒体に記録する情報記録装置に含まれる記録コンピュータを、

前記記録情報を前記画像情報単位とは異なる暗号化単位の境界において暗号鍵を変更した暗号化情報を生成する第1生成手段、

前記暗号化情報における前記画像情報単位に含まれる静止画像情報の解読に複数の暗号鍵が必要か否かを示す鍵変更情報を記録する第2生成手段、

として機能させることを特徴とする情報記録用プログラム。

【請求項 20】

少なくとも一の画像情報単位により構成される記録情報を、当該画像情報単位とは異なる暗号化単位の境界において暗号鍵を変更しつつ暗号化して得られた暗号化情報が記録されている暗号化情報記録領域と、前記暗号化情報における前記画像情報単位に含まれる静止画像情報の解読に複数の暗号鍵が必要か否かを示す鍵変更情報が記録される鍵変更情報記録領域と、が記録されている情報記録媒体から前記記録情報を再生する情報再生装置に含まれる再生コンピュータを、

前記情報記録媒体から前記暗号化情報を検出する暗号化情報検出手段、

前記情報記録媒体から前記鍵変更情報を検出する鍵変更情報検出手段、

検出された前記鍵変更情報に基づいて前記暗号化情報を解読する解読手段、

解読した前記暗号化情報を再生する再生手段、

として機能させることを特徴とする情報再生用プログラム。

【請求項 21】

請求項 19 に記載の情報記録用プログラムが前記記録コンピュータで読取可能に記録されていることを特徴とするプログラム記録媒体。

【請求項 22】

請求項 20 に記載の情報再生用プログラムが前記再生コンピュータで読取可能に記録されていることを特徴とするプログラム記録媒体。

【書類名】明細書

【発明の名称】情報記録装置及び情報記録方法、情報再生装置及び情報再生方法、情報記録用プログラム、情報再生用プログラム、情報記録媒体並びに記録媒体

【技術分野】

【0001】

本願は、情報記録装置及び情報記録方法、情報再生装置及び情報再生方法、情報記録用プログラム、情報再生用プログラム、情報記録媒体並びに記録媒体の技術分野に属し、より詳細には、映画等の動画像情報を構成する静止画情報を少なくとも含む記録情報を暗号化して情報記録媒体に記録する情報記録装置及び情報記録方法、当該暗号化して記録されている記録情報を当該情報記録媒体から再生する情報再生装置及び情報再生方法、当該情報記録に用いられる情報記録用プログラム、当該情報再生に用いられる情報再生用プログラム、当該記録情報が記録されている情報記録媒体並びに当該情報記録用プログラム又は情報再生用プログラムが記録された記録媒体の技術分野に属する。

【背景技術】

【0002】

従来、例えば放送電波を受信して得られたデジタル化された動画像情報をブロック単位で暗号化して記録する装置として、下記特許文献1に開示された暗号化装置がある。かかる暗号化装置は、暗号化に用いられる暗号化鍵を上記ブロック毎に変更するものであって、先ず入力された動画像情報をブロック分割手段で第1のブロックと第2のブロックとに分割し、上記第1のブロックを第1の暗号化手段が第2の中間データを用いて暗号化し、その暗号化結果である第1の暗号化データを出力する。

【0003】

次に、第2の暗号化手段が、第1の中間データを用い、上記第2のブロックを暗号化し、その暗号化結果である第2の暗号化データを出力する。

【0004】

その後、ブロック結合手段により、上記出力された第1の暗号化データと第2の暗号化データを結合し、元の動画像情報を暗号化した暗号化情報として出力する構成となっている。

【特許文献1】特開2000-261423

【発明の開示】

【発明が解決しようとする課題】

【0005】

しかしながら、暗号化されて記録された例えばMPEG (Moving Picture Expert Group) トランスポートストリーム (以下、適宜TS (Transport Stream) と称する) 等のデジタル情報を上記特許文献1に開示された発明を用いて再生する場合を考えると、上記MPEG トランスポートストリームにおける最小のアクセス単位であるGOP (Group Of Picture) と同一の暗号化鍵を用いて暗号化される情報単位とが相違していることに起因して、暗号化された同一のGOP内の例えばI (Intra-coded) ピクチャを再生する際に複数の異なる復号化鍵が用いられる形態で当該MPEG トランスポートストリームが記録されている場合においては、例えば早送り再生時や再生位置のサーチ時等に、当該Iピクチャに対する各暗号化鍵の適用範囲の算出処理を複数の暗号化鍵について再生処理と並行して実行しなければならないこととなり、結果として円滑な再生処理に支障を来す場合があった。

【0006】

すなわち、上記特許文献1の発明等を用いる暗号化の場合、その暗号化鍵の適用範囲はいわゆるCBC (Cipher Block Chain:暗号ブロック連鎖方式) 方式の暗号化における暗号化単位であるCBCブロックの数を用いて管理されている場合が多いのに対し、MPEG トランスポートストリームのデータの記録態様は、その情報量 (バイト数又はパケット数) を基準として管理されており、結果として上記暗号化鍵が適用される範囲と上記MPEG トランスポートストリームのデータとの間を関係付ける情報は従来から存在していな

い。

【0007】

したがって、暗号化鍵の適用範囲（換言すれば、適用切り替わり時点）を算出するには、上記MP E Gトランスポートストリームのデータを読みながら、その管理ファイル内に記述されている管理情報に基づいて逐一その適用範囲を割り出していかなければならず、上述した早送り再生時や再生位置のサーチ時等の特殊再生時における処理遅延等の支障の原因になると共に、ハードウェア的に見ても処理負荷が大きく、且つその再生処理用のメモリにおける記憶容量を大きくせざるを得ないという問題等が一例として挙げられる。

【0008】

そこで、本願は、上記の各事情を考慮して為されたもので、その課題の一例は、暗号化鍵の適用範囲（適用切り替わり時点）を逐一算出する必要をなくし、円滑な再生処理及び記録処理等を実現することが可能な情報記録装置及び情報記録方法、当該記録された情報を再生する情報再生装置及び情報再生方法、当該記録に用いられる情報記録用プログラム、当該再生に用いられる情報再生用プログラム、当該情報が記録されている情報記録媒体並びに当該情報記録用プログラム又は情報再生用プログラムが記録された記録媒体の技術分野を提供することにある。

【課題を解決するための手段】

【0009】

上記の課題を解決するため、請求項1に記載の発明は、少なくとも一の画像情報単位により構成される記録情報を、当該画像情報単位と異なる暗号化単位の境界において暗号鍵を変更しつつ暗号化して得られた暗号化情報が記録されている暗号化情報記録領域と、前記暗号化情報における前記画像情報単位に含まれる静止画像情報の解読に複数の暗号鍵が必要か否かを示す鍵変更情報が記録されている鍵変更情報記録領域と、を備える。

【0010】

上記の課題を解決するために、請求項6に記載の発明は、少なくとも一の画像情報単位により構成される記録情報を当該画像情報単位とは異なる暗号化単位の境界において暗号鍵を変更した暗号化情報を生成する第1生成手段と、前記暗号化情報における前記画像情報単位に含まれる静止画像情報の解読に複数の暗号鍵が必要か否かを示す鍵変更情報を記録する第2生成手段と、を備える。

【0011】

上記の課題を解決するために、請求項11に記載の発明は、少なくとも一の画像情報単位により構成される記録情報を、当該画像情報単位とは異なる暗号化単位の境界において暗号鍵を変更しつつ暗号化して得られた暗号化情報が記録されている暗号化情報記録領域と、前記暗号化情報における前記画像情報単位に含まれる静止画像情報の解読に複数の暗号鍵が必要か否かを示す鍵変更情報が記録される鍵変更情報記録領域と、が記録されている情報記録媒体から前記記録情報を再生する情報再生装置であって、前記情報記録媒体から前記暗号化情報を検出する暗号化情報検出手段と、前記情報記録媒体から前記鍵変更情報を検出する鍵変更情報検出手段と、検出された前記鍵変更情報に基づいて前記暗号化情報を解読する解読手段と、解読した前記暗号化情報を再生する再生手段と、を備える。

【0012】

上記の課題を解決するために、請求項17に記載の発明は、少なくとも一の画像情報単位により構成される記録情報を当該画像情報単位とは異なる暗号化単位の境界において暗号鍵を変更した暗号化情報を生成する第1生成工程と、前記暗号化情報における前記画像情報単位に含まれる静止画像情報の解読に複数の暗号鍵が必要か否かを示す鍵変更情報を記録する第2生成工程と、を備える。

【0013】

上記の課題を解決するために、請求項18に記載の発明は、少なくとも一の画像情報単位により構成される記録情報を、当該画像情報単位とは異なる暗号化単位の境界において暗号鍵を変更しつつ暗号化して得られた暗号化情報が記録されている暗号化情報記録領域と、前記暗号化情報における前記画像情報単位に含まれる静止画像情報の解読に複数の暗

号鍵が必要か否かを示す鍵変更情報が記録される鍵変更情報記録領域と、が記録されている情報記録媒体から前記記録情報を再生する情報再生方法であって、前記情報記録媒体から前記暗号化情報を検出する暗号化情報検出工程と、前記情報記録媒体から前記鍵変更情報を検出する鍵変更情報検出工程と、検出された前記鍵変更情報に基づいて前記暗号化情報を解読する解読工程と、解読した前記暗号化情報を再生する再生工程と、を備える。

【0014】

上記の課題を解決するために、請求項19に記載の発明は、少なくとも一の画像情報単位により構成される記録情報を情報記録媒体に記録する情報記録装置に含まれる記録コンピュータを、前記記録情報を前記画像情報単位とは異なる暗号化単位の境界において暗号鍵を変更した暗号化情報を生成する第1生成手段、前記暗号化情報における前記画像情報単位に含まれる静止画像情報の解読に複数の暗号鍵が必要か否かを示す鍵変更情報を記録する第2生成手段、として機能させる。

【0015】

上記の課題を解決するために、請求項20に記載の発明は、少なくとも一の画像情報単位により構成される記録情報を、当該画像情報単位とは異なる暗号化単位の境界において暗号鍵を変更しつつ暗号化して得られた暗号化情報が記録されている暗号化情報記録領域と、前記暗号化情報における前記画像情報単位に含まれる静止画像情報の解読に複数の暗号鍵が必要か否かを示す鍵変更情報が記録される鍵変更情報記録領域と、が記録されている情報記録媒体から前記記録情報を再生する情報再生装置に含まれる再生コンピュータを、前記情報記録媒体から前記暗号化情報を検出する暗号化情報検出手段、前記情報記録媒体から前記鍵変更情報を検出する鍵変更情報検出手段、検出された前記鍵変更情報に基づいて前記暗号化情報を解読する解読手段、解読した前記暗号化情報を再生する再生手段、として機能させる。

【0016】

上記の課題を解決するために、請求項21に記載の発明は、請求項19に記載の情報記録用プログラムが前記記録コンピュータで読取可能に記録されている。

【0017】

上記の課題を解決するために、請求項22に記載の発明は、請求項20に記載の情報再生用プログラムが前記再生コンピュータで読取可能に記録されている。

【発明を実施するための最良の形態】**【0018】**

以下、本願の実施の形態について、図面を参照しながら説明する。

【0019】

なお、以下に説明する実施の形態は、BS (Broadcasting Satellite) デジタル放送に代表されるようなデジタル放送にて配信されるAV (Audio Visual) 情報を上記CBC方式に則って暗号化した上でハードディスク等の情報記録媒体に記録することが可能とされている情報記録装置、及び上記AV情報の再生処理が可能とされている情報再生装置に対して夫々本願を適用した場合の実施の形態である。なお、以下の説明では、後述のハードディスク1を共通として一つの筐体に収められている情報記録装置と情報再生装置とを別個に説明する。

【0020】

また、以下の説明において、上記AV情報は、動画像の圧縮技術に関する規格として周知のMP EG 2規格におけるトランスポートストリーム規格に則って放送されてくるものとする。

【0021】

さらに、以下に説明する記録処理及び再生処理においては、上記暗号化単位としてのCBCブロックに適用される規格、ハードディスクや記録メディアの物理的なアクセス単位に適用される規格、及び上記アクセス単位の情報記録媒体上におけるアクセス開始位置と上記CBCブロックの当該情報記録媒体上の先頭位置とを合致させることに関する規格は基本的に最低限遵守されるものとする。

【0022】

上記各規格についてより具体的には、記録されているAV情報に含まれている各コンテンツに対するアクセスは、そのアクセス位置を含むハードディスク等におけるセクタの先頭から行われるものとされている。

【0023】

また、例えばハードディスク等の物理的なアクセス単位の情報量が512バイトであって、論理的にその倍数、例えば6144（12倍）バイト毎にしかアクセスしない場合には、CBCブロックの情報量をそのアクセス単位の情報量に合わせることになる。すなわち、ハードディスク等におけるアクセス位置とCBCブロックの開始位置とが一致しているものとする。

【0024】

(I) 記録フォーマットの実施の形態

始めに、本実施の形態に係る情報記録装置について具体的に説明する前に、当該情報記録装置により上記ハードディスクに対して上記AV情報を記録する際に用いられる論理的な記録フォーマットの概要について、図1及び図2を用いて説明する。

【0025】

なお、図1及び図2に示す記録フォーマットは、上記AV情報が当該記録フォーマットに基づいてハードディスクに記録された後の当該記録フォーマットを階層的かつ模式的に夫々示す図である。

【0026】

また、図1及び図2に示す記録フォーマットは、本実施の形態のAV情報をハードディスクに記録する際に用いられる論理的な記録フォーマットであり、当該記録の際に用いられる物理的な記録フォーマットについては、ハードディスクに用いられている周知の物理フォーマットがそのまま用いられる。

【0027】

まず、記録されているAV情報の内容及び記録態様を効率的に管理すべく当該記録フォーマットにおいて採用されている種々の概念について、その概要を説明する。

【0028】

第1に、以下の記録フォーマットにおいては、記録されているAV情報を取り扱う際の単位として、ユニットなる概念が用いられている。すなわち、当該ユニットとは、時間的に連続してハードディスクに記録された一のAV情報をいう。例えば、AV情報がBSデジタル放送で放送された場合は、当該BSデジタル放送における一のイベントが一のユニットとなるように定義されている。

【0029】

第2に、以下の記録フォーマットにおいては、例えばBSデジタル放送中において、放送配信者側の意図によってトランスポートストリーム中の映像情報を格納するパケットのパケットIDが同一である部分についてディレクトリなる概念が用いられている。すなわち、ディレクトリとは、一のユニット全体またはその一部を特定して、同一のパケットIDである区間を表すものである。

【0030】

そして、第3に、以下の記録フォーマットにおいては、ユニット中において、MPEG2規格で述べられているGOPを搬送している一の分割区間情報を示す、アプリケーションGOPなる概念が用いられている。このアプリケーションGOPは、MPEG-TSのシーケンスヘッダと、当該シーケンスヘッダに後続して送信されるGOPデータとからなり、本願の画像情報単位を構成する。また、上記アプリケーションGOPにより構成されるMPEG-TSは、本願の記録情報を構成する。さらに、Iピクチャは、本願の静止画像情報であるフレーム内符号化画像情報を構成し、GOPが本願の符号化画像情報群を構成する。

【0031】

次に、上述した種々の概念に基づいて本実施の形態に係る論理的な記録フォーマットに

ついて説明する。

【0032】

図1に示すように、必要なAV情報が記録された後のハードディスク1上には、上記したユニットのそれぞれに対応する管理情報であるユニット情報2と、放送されハードディスク1に記録されているAV情報の実態そのものであるAVストリーム情報3と、が記録されている。このAVストリーム情報3は、本願の暗号化情報記録領域を構成する。

【0033】

また、上記ユニット情報2は、暗号化情報4と、上記AVストリーム情報3を管理するための管理情報であるストリーム情報5と、から構成されている。

【0034】

ここで、当該ストリーム情報5は、ユニットの中に含まれるTSパケットの数を示すユニットサイズ6（4バイト）と、ユニット中に含まれるアプリケーションGOPの数を示すポインタテーブル数7（4バイト）と、各アプリケーションGOPの情報を示すポインタテーブル8（アプリケーションGOPの数（図1の場合はm個）だけ含まれている）と、により構成されている。

【0035】

次に、上記ポインタテーブル8の細部構成について、図1及び図2を用いて説明する。

【0036】

図1に示すように、一のポインタテーブル8は、対応するアプリケーションGOPに含まれるパケット数を示すGOPサイズ9（4バイト）と、対応するアプリケーションGOPの最初のパケットから数えてアプリケーションGOPの中にある最初のIピクチャを包含し終えるパケットまでの数を示す第1参照画像サイズ10（2バイト）と、上記最初のIピクチャが記録されている領域において復号の際に暗号化鍵の変更が必要である旨を表す鍵変更フラグ11（1バイト）と、により構成されている。この鍵変更フラグ11は、本願の鍵変更情報記録領域を構成し、アプリケーションGOP毎に設けられている。

【0037】

ここで、鍵変更フラグ11は、GOPのIピクチャを復号するために複数の暗号化鍵が必要であることを示すフラグであり、当該複数の暗号化鍵が復号に必要である場合にはその値が「1」とされ、一の暗号化鍵のみでそのIピクチャが復号できる場合又はそもそも復号が必要でない場合にはその値が「0」とされるものである。すなわち、鍵変更フラグ11は、暗号化して記録したMPEG-TSにおけるアプリケーションGOPに含まれるIピクチャの解読に複数の鍵が必要か否かを示す鍵変更情報が記録されている。

【0038】

一方、暗号化情報4は、図2に示すように、上記ユニットを復号しながら再生するために必要な、元のユニットの暗号化に関する情報であり、当該ユニットを復号しながら再生するための暗号化鍵の適用範囲数を示す適用数Eと、夫々の適用範囲に関する情報である適用範囲情報12（各暗号化鍵の適用範囲の数だけ含まれている）と、から構成されている。

【0039】

また、各適用範囲情報12は、その適用範囲内を実際に復号するために用いられる暗号化鍵Kと、対応する暗号化鍵Kの適用開始位置を、AVストリーム情報3の先頭からのCBCブロックの数で表した適用開始CBC番号13と、各適用範囲の大きさをCBCブロックの数で示す適用CBC数14と、から構成されている。

【0040】

(II) 情報記録装置の実施の形態

次に、上述した記録フォーマットを前提としてAV情報をハードディスクに記録する情報記録装置の構成及び動作について説明する。

【0041】

まず、図3を用いて当該情報記録装置の全体構成及び概要動作について説明する。なお、図3において、CPU25は情報記録装置20内の全ての構成要素をコントロールする

ものの、簡単のため本実施の形態に係るコントロール部分のみを図示している。

【0042】

図3に示すように、本実施の形態の情報記録装置20は、外部にあるテレビジョン装置TVに直接接続されているとともに、デジタル放送がアンテナにより受信される図示しないデジタル放送受信回路に接続されている。

【0043】

また、情報記録装置20は、デマルチプレクサ21と、映像音声データデコーダ22と、プレイバックモジュール23と、レコードモジュール24と、第1生成手段、第2生成手段及CPU25と、メモリ26と、IDEコントローラ27と、バス28と、情報記録媒体としてのハードディスク（以下、適宜HDと称する）1と、により構成されている。

【0044】

次に、概要動作について説明する。

【0045】

先ず、デマルチプレクサ21は、上記デジタル放送受信回路から入力されたMPEG-TSから必要なパケットのみを抽出する。より具体的には、デマルチプレクサ21は、MPEG-TSの形式で送信されてくるデジタル放送中からデコードすべき映像信号を搬送しているパケットIDを指定することによって、そのビデオ信号のパケットを通過させる。同様に、オーディオ信号やその他の付加的なデータ、その他のCPU25で用いるデータを搬送しているパケットIDが設定されると、そのパケットIDにより示されるパケットを抽出する機能をも備えている。このようにMPEG-TS形式で搬送されてきた情報の中から必要なパケットのみを抽出したものをパーシャルTSと呼ぶことにする。

【0046】

次に、映像音声データデコーダ22は、デマルチプレクサ21により得られたパーシャルTSからCPU25によって指定されたパケットIDで搬送されている音声及び映像情報をデコードし、また付加的なデータを抽出し、これらを映像データと音声データとして出力する機能を有する。

【0047】

一方、プレイバックモジュール23は、HD1に記録されているパーシャルTSを、IDEコントローラ27を用いてデマルチプレクサ21にデータを供給する。

【0048】

他方、レコードモジュール24は、パーシャルTSを暗号化しながらIDEコントローラ27を用いてHD1に暗号化ストリームを記録する。

【0049】

これらの処理と並行して、CPU25は、上記した全ての構成要素を制御する。このとき、揮発性のメモリ26は、情報記録の際にはHD1のユニット情報2に相当する情報をその中に構築し、一方、情報再生の際には当該ユニット情報2を一時的に記憶する。

【0050】

また、IDEコントローラ27は、ATA（AT Attachment）のコマンドを発行してHD1とデータ授受を行う。

【0051】

次に、レコードモジュール24の内部構成を、図4に用いて説明する。

【0052】

図4に示すように、レコードモジュール24は、パーシャルTSを取得する情報供給部31と、暗号化ストリームを出力する暗号化部32と、から構成され、さらに情報供給部31は、外部から得られた情報を後段の暗号化部32に供給し、その際、バッファリング等の処理を行う。

【0053】

また、情報供給部31は、CPU25からの制御信号に基づいて、それらの動作を開始又は停止する機能を有している。さらに情報供給部31には、特定の単位情報を識別したか否かの状態（より具体的には、Iピクチャの先頭又はそれに類するシーケンスヘッダコ

ード (SHC) や GOP ヘッダを検出した状態、検出後の別なピクチャの先頭の検出した後の状態等) を保持する特定単位情報識別状態フラグ 31 a が設定されており、その特定単位情報識別状態フラグ 31 a は他の構成部材から参照可能とされている。このとき、情報供給部 31 では、特定の単位情報を識別する動作を続けており、常に状態を遷移させている。そして、情報供給部 31 は、パケットカウンタ 31 b をさらに有しており、入力されたパケットをカウントし、そのカウント値を示すデータを保持する。

【0054】

一方、暗号化部 32 は、CBC ブロックの数を計数する CBC カウンタ 32 a を有し、CPU 26 からの制御信号に基づいて暗号鍵を生成し、情報供給部 31 から得られた情報を固定長の暗号ブロック毎に暗号化し、後段の手段に情報を出力する。

【0055】

なお、記録終了時点では、CPU 25 がメモリ 26 内の情報をユニット情報 2 として HD 1 に書き込む動作を行う。これにより、HD 1 内の論理情報が構築される。

【0056】

(II-A) 記録処理

次に、CPU 25 を中心とした情報記録装置 20 による記録処理について、図 5 を参照して説明する。

【0057】

CPU 25 は、ステップ S1 で初期化処理を実行する。すなわち、この初期化処理では、暗号化情報 4 の適用数 E の値を「0」、パケットカウンタ 31 b の値を「0」、前アプリケーション GOP 位置の値を「0」、CBC カウンタ 32 a の値を「0」、特定単位情報識別状態フラグ 31 a の値を「0」、アプリケーション GOP 指数の値を「0」、適用範囲情報 12 の適用開始 CBC 番号 13 の値を「0」に設定する処理を夫々に行う。

【0058】

次に、暗号化部 32 にて暗号鍵を生成して待機し、適用範囲情報 12 の鍵 K を決定し、暗号化情報 4 の適用数 E をインクリメントした後 (ステップ S2)、情報供給部 31 でいずれかのピクチャの検出動作をスタートし、パシャル TS の入力を開始する (ステップ S3)。

【0059】

ステップ S4 では、情報供給部 31 で最初のシーケンスヘッダコードを検出するまで待機し、最初のシーケンスヘッダコードを検出した場合に特定単位情報識別状態フラグ 31 a の値を「1」とする (ステップ S5)。

【0060】

ステップ S6 において、情報供給部 31 は、パケットを一つ入力し、パケットカウンタ 31 b をインクリメントした後、暗号化補助動作を実行する (ステップ S7)。なお、この暗号化補助動作については後ほど詳述する。

【0061】

ステップ S8 では、CPU 25 は、情報供給部 31 で次のピクチャが検出されたか否かを判定し、次のピクチャが検出された場合 (ステップ S8; YES) には、ステップ S9 に進み、特定単位情報識別状態フラグ 31 a の値を「0」とする。一方、次のピクチャが検出されない場合 (ステップ S8; NO) には、ステップ S6 に戻り、次のピクチャが検出されるまで、ステップ S6 及びステップ S7 の処理を繰り返す。

【0062】

次に、ステップ S10 では、パケットカウンタ 31 b の値から前アプリケーション GOP 位置の値を減算し、対応するアプリケーション GOP 内の第 1 参照画像サイズ 10 に格納し、ステップ S6 及びステップ S7 と同様にステップ S11 でパケットを一つ入力し、パケットカウンタ 31 b の値をインクリメントした後、上記暗号化補助動作を再度実行する (ステップ S12)。

【0063】

次に、ステップ S13 において、CPU 25 は、シーケンスヘッダコードが検出された

か否かを判定し、当該シーケンスヘッダコードが検出された場合（ステップS13；YES）には、ステップS14に進み、パケットカウンタ31bの値から前アプリケーションGOP位置の値を減算して対応するアプリケーションGOP内のGOPサイズ9に格納する。一方、シーケンスヘッダコードが検出されない場合（ステップS13；NO）には、ステップS11に戻り、シーケンスヘッダコードが検出されるまで、ステップS11及びステップS12の処理を繰り返す。

【0064】

これにより、ステップS15では、アプリケーションGOPの番号を示すパラメータiをインクリメントした後、パケットカウンタ31bの値を前アプリケーションGOP位置の値に格納する（ステップS16）。そして、ステップS5に戻り、当該ステップS5以下の処理を繰り返す。

【0065】

（II-B）暗号化補助動作処理

次に、CPU25による上記暗号化補助動作処理の詳細について、図6を用いて説明する。

【0066】

当該暗号化補助動作処理において、CPU25は、先ずステップS21で特定単位情報識別状態フラグ31aが「1」であるか否かを判定し、特定単位情報識別状態フラグ31aの値が「1」である場合（ステップS21；YES）には、ステップS22で新しい暗号鍵が生成されたか否か次に判定する。そして、新しい暗号鍵が生成された場合（ステップS22；YES）には、一つ前（E-1番目）の適用範囲情報12内の適用CBC数14の値を、そのときのCBCカウンタ32aの値から当該一つ前（E-1番目）の適用範囲情報12内の適用開始CBC番号13の値を減算した値とし（ステップS23）、さらに、E番目の適用範囲情報12内の適用開始CBC番号13の値を、そのときのCBCカウンタ32aの値とし（ステップS24）、その後に適用数Eをインクリメントする（ステップS25）。

【0067】

ステップS26では、図示しない暗号化バッファ内にデータがあるか否かを判定し、データがある場合（ステップS26；YES）には、ステップS27でi番目のアプリケーションGOPにおける鍵変更フラグ11の値を「1」とした後、ステップS28に進む。

【0068】

なお、ステップS21で特定単位情報識別状態フラグ31aの値が「1」でない場合（ステップS21；NO）、ステップS22で新しい暗号鍵が生成されない場合（ステップS22；NO）及びステップS26で暗号化バッファ内にデータがない場合（ステップS26；NO）には、それぞれ直接ステップS28に進む。

【0069】

そして、ステップS28では、暗号化バッファ内のデータの情報量が一のCBCブロックの情報量に到達したか否かを判定し、そのデータの情報量が一のCBCブロックの情報量に達した場合（ステップS28；YES）には、ステップS29において対応するCBC単位で暗号化した後、CBCカウンタ32aをインクリメントして暗号化後の情報を記録する（ステップS30、S31）。

【0070】

なお、ステップS28で、蓄積されているデータ量が、CBCブロックの情報量に達していない場合（ステップS28；NO）には、ステップS21に戻る。これら一連の処理を実行することにより、暗号化補助動作を終了する。

【0071】

（II-C）RAMに展開された記録フォーマットの実施の形態

次に、本実施の形態において、図3に示すメモリ26がRAMであって、当該メモリ26に展開されたストリーム情報5を図7を用いて、メモリ26に展開された暗号化情報4を図8を用いて、夫々説明する。なお、図7及び図8において、図1及び図2と同一の部

分には、同一の符号を付してその説明を省略する。

【0072】

本実施の形態では、記録処理を実行する際、メモリ26内に必要なユニット情報2が展開されつつ構築される。

【0073】

すなわち、メモリ26内に設定されるストリーム情報一時記憶領域36に展開されたストリーム情報5は、図7に示すように、図1と同様にユニットの中に含まれるTSパケットの数を示すユニットサイズ6と、ユニット中に含まれるアプリケーションGOPの数を示すポインタテーブル数7と、アプリケーションGOPの情報を示すポインタテーブル8と、により構成されている。

【0074】

また、同じくメモリ26内に設定される暗号化情報一時記憶領域35に展開された暗号化情報4は、図8に示すように、図2と同様の適用数Eと、夫々の適用範囲に関する情報である適用範囲情報12と、から構成されている。

【0075】

(II-D) 記録終了処理

次に、CPU25を中心としてHD1への一連の記録処理を終了する際に実行される記録終了処理について、図9を用いて説明する。

【0076】

当該記録終了処理においては、まず、CPU25は、暗号化情報一時記憶領域35から暗号化情報4を、ストリーム情報一時記憶領域36からストリーム情報5を、夫々読み出してユニット情報2として記録し(ステップS35)、全ての記録動作を終了する(ステップS36)。

【0077】

(III) 情報再生装置の実施の形態

次に、上述した記録フォーマットを用いてHD1に記録されているAVストリーム情報3を再生する情報再生装置の構成及び動作について説明する。

【0078】

まず、図10を用いて当該情報再生装置の全体構成及び概要動作について説明する。

【0079】

図10に示すように、本実施の形態の情報再生装置40は、情報出力部41と、鍵変更情報検出手段、解読手段及び検索手段としての非暗号化部42と、暗号化情報検出手段及び再生手段としての読出し部43とから構成されている。非暗号化部42は、検出された鍵変更情報が、暗号化されたIピクチャを解読する処理において二以上の鍵Kが必要であることを示す場合は、当該Iピクチャの解読に必要な鍵Kを検索する。また、読出し部43は、上記HD1から得られた暗号化された情報(暗号化されたパーシャルTS)を非暗号化部42に出力する。

【0080】

これにより、非暗号化部42は、図示しないCPUからの制御によって読出し部43から得られたパーシャルTSを上記CBCブロック毎に解読し、情報出力部41に復号されたパーシャルTSとして出力する。

【0081】

そして、情報出力部41は、非暗号化部42から得られた復号後のパーシャルTSを、予め設定されたバッファ処理等を実行しつつ外部に供給する。また、情報出力部41は、図示しないCPUからの制御によって、それらの動作を開始及び停止する機能を有している。

【0082】

(III-A) 通常再生処理

次に、図示しないCPUによる通常再生処理について、図11を用いて説明する。なお、当該再生処理は、HD1に記録されているAVストリーム情報3の先頭から通常再生す

る処理である。

【0083】

まず、ステップS41で情報取得アドレスを「0」にした後、再生処理を中止する操作が図示しない操作部において実行されたか否かを判定し（ステップS42）、その操作が実行された場合（ステップS42；YES）には、再生処理を終了する。

【0084】

一方、再生処理の中止操作が実行されない場合（ステップS42；NO）には、ステップS43に進み、情報取得アドレスの位置からAVストリーム情報3を取得する。

【0085】

次いで、ステップS44では、情報取得アドレスに相当するCBCブロックの適用範囲を検索し、その検索結果から適用範囲情報12を取得し、鍵Kを得る（ステップS45）。なお、当該ステップS44の処理については、後述する。

【0086】

そして、ステップS46では、読出し部43から得られたパーシャルTSを非暗号化部42により固定長のCBCブロック毎に鍵Kを用いて復号した後、情報取得アドレスをインクリメントする（ステップS47）。以下、ステップS42で再生が中止されるまでステップS43からステップS47までの処理を繰り返す。

【0087】

なお、情報取得アドレスに相当する適用範囲を検索するため、図2に示す暗号化情報4内の適用範囲情報12を順次参照する動作が発生する。但し、図11に示す通常再生の場合は、情報取得アドレスをCBCブロックの情報量の定数倍としてもよく、このようにCBCブロックの情報量の定数倍とした場合には、CBCブロックの適用範囲の検索が容易になる。

【0088】

(III-B) 適用範囲検索処理

次に、上記ステップS44としての適用範囲検索処理について、図12を用いて詳説する。なお、当該適用範囲検索処理は、AVストリーム情報3内のアクセス位置（CBC数）に換算し、現在どの鍵Kが必要かを検索するルーチンである。

【0089】

まず、ステップS51でAVストリーム情報3内のアクセス位置（バイト数）PをCBCブロックの情報量で除して現在のアクセス位置（CBC数）pを求めた後、パラメータiを「1」とする（ステップS52）。ここで、図12において、パラメータiはCBC換算での適用範囲の番号を示すパラメータである。

【0090】

次いで、ステップS53では、パラメータiが暗号化情報4の適用数E未満であるかを判定し、パラメータiが適用数E未満の場合（ステップS53；YES）には、ステップS54でアクセス位置（CBC数）pがCBCブロック換算でi番目の適用範囲x（i）以上であるかを判定し、適用範囲x（i）以上の場合（ステップS54；YES）には、ステップS55でそのアクセス位置（CBC数）pが、「適用範囲x（i）+適用サイズy（i）」未満であるかを判定し、「適用範囲x（i）+適用サイズy（i）」未満の場合（ステップS55；YES）には、ステップS56でメインルーチンに戻るときの戻り値を「i」として検索処理を終了する。

【0091】

一方、ステップS53で適用数Eがパラメータi以上の場合（ステップS53；NO）には、ステップS57で戻り値を「1」だけデクリメントして検索処理を終了する。

【0092】

また、ステップS54で適用範囲x（i）がアクセス位置（CBC数）pの外である場合（ステップS54；NO）、及びステップS55で「適用範囲x（i）+適用サイズy（i）」がアクセス位置（CBC数）pの外である場合（ステップS55；NO）には、ステップS58でパラメータiをインクリメントしてステップS53に戻る。

【0093】

(III-C) 特殊再生処理(C-1) 第1特殊再生処理

次に、図示しないCPUによる、通常再生以外の特殊再生処理について、図13を用いて説明する。

【0094】

なお、図13に示す特殊再生処理は、鍵変更フラグ11を参照しながら動作する、早送り再生又は検索処理等の特殊再生ルーチンである。

【0095】

まず、ステップS61では、最初のディレクトリにおいて最初のポインタテーブルを参照するように初期化する。

【0096】

ステップS62では、最初のIピクチャの位置を、「最初のディレクトリのパケットポインタ(バイト)+GOPパケットポインタ(パケット数)×パケットサイズ(バイト)」を情報取得アドレスN(バイト)として求める。

【0097】

ステップS62では、特殊再生終了指示があったか否かを判定し、特殊再生終了指示があった場合(ステップS62; YES)には、特殊再生処理を終了する。一方、特殊再生終了指示がない場合(ステップS62; NO)には、ステップS64に進み、第1参照画像サイズ10から読込バイト数Mを取得した後、情報取得アドレスNに相当する鍵Kの適用範囲を検索する(ステップS65)。

【0098】

ステップS66では、図示しないCPUは鍵変更フラグ11が「0」でないかを判定し、鍵変更フラグ11が「0」でない場合(ステップS66; YES)には、「情報取得アドレスN+読込バイト数M」の位置にあるデータを復号するための鍵Kの適用範囲を検索して復号する(ステップS67, S68)。なお、鍵変更フラグ11が「0」の場合(ステップS66; NO)には、直接ステップS68に進んで復号する。

【0099】

ステップS69では、情報取得アドレスNに「GOPサイズ(パケット数)×パケットサイズ」を加算して情報取得アドレスNを変更した後、次のポインタテーブル8を参照するように変更する(ステップS70)。

【0100】

そして、これ以後、ステップS63で特殊再生終了指示があるまでステップS64からステップS70までの処理を繰り返す。

【0101】

(C-2) 第2特殊再生処理

次に、図示しないCPUによる第2特殊再生処理について、図14を用いて説明する。

【0102】

なお、図14に示す第2特殊再生処理は、適用範囲情報12の最適化を行って検索ルーチンを省いた特殊再生ルーチンである。また、図13に示す第1特殊再生処理と同一の処理は、同一のステップ番号を付してその説明を省略する。

【0103】

図14に示す第2特殊再生処理は、ステップS66で鍵変更フラグ11が「0」でないかを判定し、鍵変更フラグ11が「0」でない場合(ステップS66; YES)には、ステップS67aにおいて次の適用範囲情報12を得るようにしている。

【0104】

ここで、仮に上記適用範囲情報12がアクセスする順に並んでいるとし、且つ適用範囲12の間に空隙がないとするならば、図13に示す第1特殊再生処理のように「情報取得アドレスN+読込バイト数M」からの適用範囲検索を省略し、現在アクセスしている適用範囲情報12の次の適用範囲情報12をアクセスするようにしてもよい。

【0105】

(IV) 鍵変更フラグの他の実施形態

次に、鍵変更フラグ11の他の実施形態について、図15を用いて説明する。なお、図15は、鍵変更フラグ11の拡張を示す説明図である。なお、図15(A)及び(B)において、ハッチング部分は、鍵Kが変更されていることを示している。

【0106】

上述した実施形態においては、鍵変更フラグ11を1バイトの情報として説明したが、これ以外に、鍵変更フラグを、一のアプリケーションGOP内において鍵Kが変更されたか否かを示す前半四ビットの情報と、一のIピクチャの復号中に鍵Kが変更されるか否かを示す後半四ビットの情報とで、構成するように拡張することもできる。

【0107】

この場合、前半四ビットの情報につき、値「0000b」(bは二進数であることを示す。以下、同様)は対応するアプリケーションGOP再生中に鍵Kの変更が必要無いことを示し、値「0001b」は対応するアプリケーションGOP再生中に鍵Kの変更が必要であることを示し、値「0010b」は対応するアプリケーションGOP再生中にAVストリーム情報3の終了点が存在することを示し、値「0011b」は対応するアプリケーションGOP再生中にAVストリーム情報3の開始点が存在することを示すものと定義づける。

【0108】

一方、後半四ビットの情報につき、値「0000b」は対応するIピクチャの読み込みに鍵Kの変更が必要無いことを示し、値「0001b」は対応するIピクチャの読み込みに鍵Kの変更が必要であることを示し、値「0010b」は対応するIピクチャの途中でAVストリーム情報3の終了点が存在することを示し、値「0011b」は対応するIピクチャの途中でAVストリーム情報3の開始点が存在することを示すものと定義づける。

【0109】

このように定義付けて鍵変更フラグを上記実施形態のように用いれば、例えば、図15(A)に示すようにアプリケーションGOPの途中であって、Iピクチャの途中で鍵Kの変更位置がある場合は、鍵変更フラグの値を「0001b-0001b」として表現できる。

【0110】

また、図15(B)に示すようにアプリケーションGOPの途中で鍵Kの変更位置があるものの、Iピクチャの途中には鍵Kの変更位置がない場合は、鍵変更フラグの値を「0001b-0000b」として表現できる。

【0111】

さらに、図15(C)に示すように、アプリケーションGOPの途中であって、Iピクチャの途中から暗号化されていない場合は、鍵変更フラグの値を「0010b-0010b」として表現できる。

【0112】

最後に、図15(D)に示すように、アプリケーションGOPの途中から暗号化されているがIピクチャは暗号化されていない場合は、鍵変更フラグの値を「0011b-0000b」として表現できる。

【0113】

このように、図15(A)乃至(D)に示すように、IピクチャだけでなくアプリケーションGOP中に鍵Kの変更位置が存在する場合でも鍵変更フラグを用いて表現することができるのである。

【0114】

以上説明したように、本実施の形態のHD1によれば、アプリケーションGOPにより構成されるMP EG2規格におけるトランスポートストリームを、当該アプリケーションGOPと異なるCBCブロックの境界において暗号鍵を変更しつつ暗号化して得られた暗号化情報が記録されているAVストリーム情報3と、上記暗号化情報におけるアプリケー

ションGOPに含まれるIピクチャの解読に複数の暗号鍵が必要か否かを示す鍵変更情報が記録されている鍵変更フラグ11と、が記録されているので、鍵Kの適用切り替わり時点を逐一算出する必要がなくなり、円滑な処理を実行することができるとともに、ハードウェア的な負荷を小さく、且つメモリ26の容量を少なくすることができる。

【0115】

また、鍵変更フラグ11は、アプリケーションGOP毎に設けられているので、鍵Kの適用切り替わり時点を逐一算出する必要がなくなり、円滑な処理を実行することができるとともに、ハードウェア的な負荷を小さく、且つメモリ26の容量を少なくすることができる。

【0116】

さらに、静止画像情報としてIピクチャを解読するので、鍵Kの適用切り替わり時点を逐一算出する必要がなくなり、円滑な処理を実行することができるとともに、ハードウェア的な負荷を小さく、且つメモリ26の容量を少なくすることができる。

【0117】

そして、アプリケーションGOPは、MPEG2規格におけるトランスポートストリームのシーケンスヘッダと、当該シーケンスヘッダに後続して送信されるGOPと、により構成されているので、鍵Kの適用切り替わり時点を逐一算出する必要がなくなり、円滑な処理を実行することができるとともに、ハードウェア的な負荷を小さく、且つメモリ26の容量を少なくすることができる。

【0118】

本実施の形態の情報記録装置20によれば、アプリケーションGOPにより構成されるMPEG2規格におけるトランスポートストリームを、当該アプリケーションGOPと異なるCBCブロックの境界において暗号鍵を変更した暗号化情報を生成するCPU25と、上記暗号化情報におけるアプリケーションGOPに含まれるIピクチャの解読に複数の暗号鍵が必要か否かを示す鍵変更情報を記録するCPU25と、を備えているので、情報記録装置20において鍵Kの適用切り替わり時点を逐一算出する必要がなくなり、円滑な処理を実行することができるとともに、ハードウェア的な負荷を小さく、且つメモリ26の容量を少なくすることができる。

【0119】

また、鍵変更フラグ11は、アプリケーションGOP毎に設けられているので、鍵Kの適用切り替わり時点を逐一算出する必要がなくなり、円滑な処理を実行することができるとともに、ハードウェア的な負荷を小さく、且つメモリ26の容量を少なくすることができる。

【0120】

さらに、静止画像情報としてIピクチャを解読するので、鍵Kの適用切り替わり時点を逐一算出する必要がなくなり、円滑な処理を実行することができるとともに、ハードウェア的な負荷を小さく、且つメモリ26の容量を少なくすることができる。

【0121】

そして、アプリケーションGOPは、MPEG2規格におけるトランスポートストリームのシーケンスヘッダと、当該シーケンスヘッダに後続して送信されるGOPと、により構成されているので、鍵Kの適用切り替わり時点を逐一算出する必要がなくなり、円滑な処理を実行することができるとともに、ハードウェア的な負荷を小さく、且つメモリ26の容量を少なくすることができる。

【0122】

さらにまた、本実施の形態の情報再生装置40によれば、HD1から暗号化情報を検出する読出し部43と、HD1から鍵変更情報を検出する非暗号化部42と、検出された鍵変更情報に基づいて暗号化情報を解読する非暗号化部42と、解読した暗号化情報を再生する読出し部43と、を備えているので、鍵Kの適用切り替わり時点を逐一算出する必要がなくなり、円滑な処理を実行することができるとともに、ハードウェア的な負荷を小さくすることができる。

【0123】

また、鍵変更フラグ11は、アプリケーションGOP毎に設けられているので、鍵Kの適用切り替わり時点を逐一算出する必要がなくなり、円滑な処理を実行することができるとともに、ハードウェア的な負荷を小さく、且つメモリ26の容量を少なくすることができる。

【0124】

さらに、静止画像情報としてIピクチャを解釈するので、鍵Kの適用切り替わり時点を逐一算出する必要がなくなり、円滑な処理を実行することができるとともに、ハードウェア的な負荷を小さく、且つメモリ26の容量を少なくすることができる。

【0125】

そして、アプリケーションGOPは、MPEG2規格におけるトランスポートストリームのシーケンスヘッダと、当該シーケンスヘッダに後続して送信されるGOPと、により構成されているので、鍵Kの適用切り替わり時点を逐一算出する必要がなくなり、円滑な処理を実行することができるとともに、ハードウェア的な負荷を小さく、且つメモリ26の容量を少なくすることができる。

【0126】

なお、本願は上記実施の形態に限定されることなく、種々の変更が可能である。

【0127】

例えば、上記実施の形態では、BSデジタル放送等の電波を受信して映像信号等を取得するようにしたが、これ以外にアナログ地上波TV放送の電波や、インターネット又は専用回線を介したサーバVOD (Video On Demand) から映像信号等を取得するようにしてもよい。

【0128】

また、上記実施の形態では、記録媒体としてHD1を用いた場合について説明したが、これ以外に情報の書き換えが可能なDVDやフラッシュメモリ等の各種記録媒体を使用することができる。

【0129】

さらに、図5、図6、図9、図11乃至図14に示すフローチャートに対応するプログラムを、フレキシブルディスク又はHD等の情報記録媒体に記録させておき、或いは当該プログラムをインターネット等のネットワークを介して取得した後に記録しておき、これらを汎用のマイクロコンピュータ等により読み出して実行することにより、当該マイクロコンピュータを実施の形態に係るCPU25等として機能させることが可能である。

【図面の簡単な説明】

【0130】

【図1】 本実施形態の記録フォーマットのストリーム情報を示す説明図である。

【図2】 本実施形態の記録フォーマットの暗号化情報を示す説明図である。

【図3】 本実施形態の情報記録装置の全体構成を示すブロック図である。

【図4】 レコードモジュールの内部構成を示すブロック図である。

【図5】 本実施形態の記録処理を示すフローチャートである。

【図6】 本実施形態の暗号化補助動作処理を示すフローチャートである。

【図7】 本実施形態においてRAMに展開されたストリーム情報のフォーマットを示す説明図である。

【図8】 本実施形態においてRAMに展開された暗号化情報のフォーマットを示す説明図である。

【図9】 本実施形態の記録終了処理を示すフローチャートである。

【図10】 本実施形態の情報再生装置を示すブロック図である。

【図11】 本実施形態の再生処理を示すフローチャートである。

【図12】 本実施形態の検索処理を示すフローチャートである。

【図13】 本実施形態の特殊再生処理を示すフローチャートである。

【図14】 本実施形態の他の特殊再生処理を示すフローチャートである。

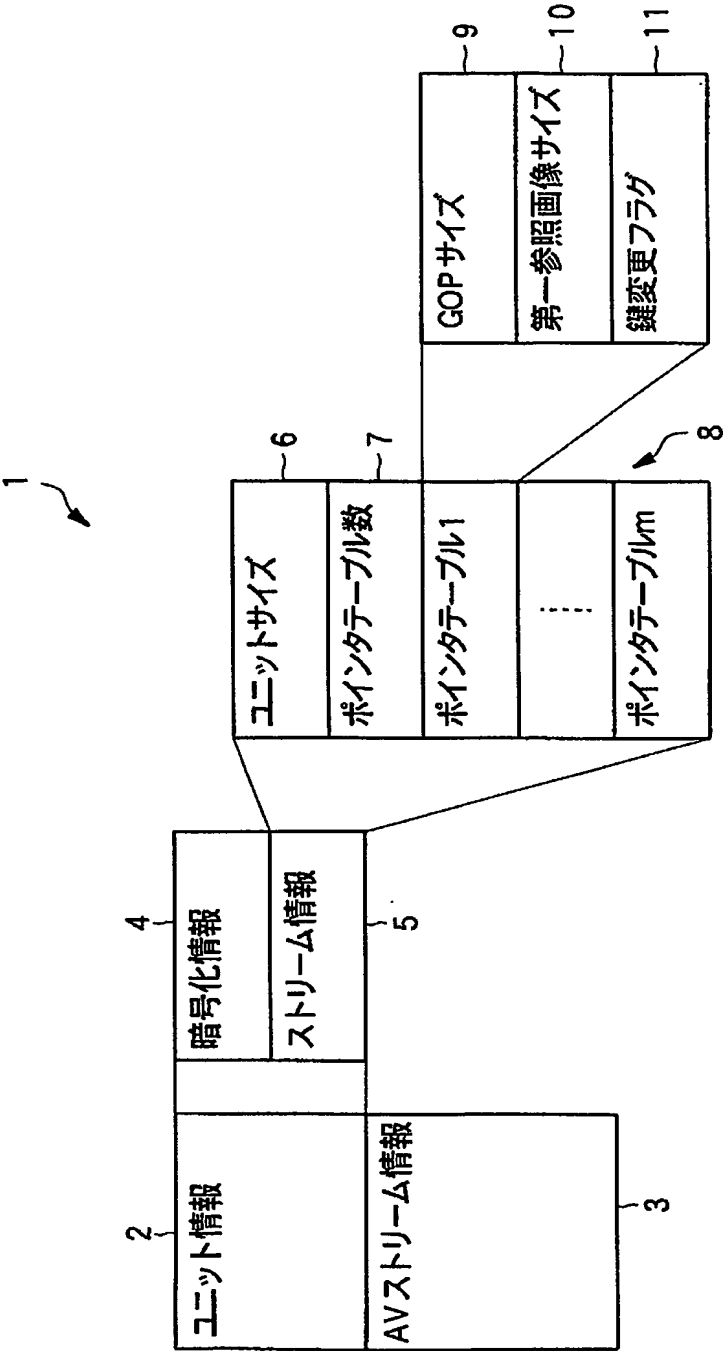
【図15】本実施形態の鍵変更フラグの拡張態様を示す説明図であり、(A)は第1の例を示す図であり、(B)は第2の例を示す図であり、(C)は第3の例を示す図であり、(D)は第4の例を示す図である。

【符号の説明】

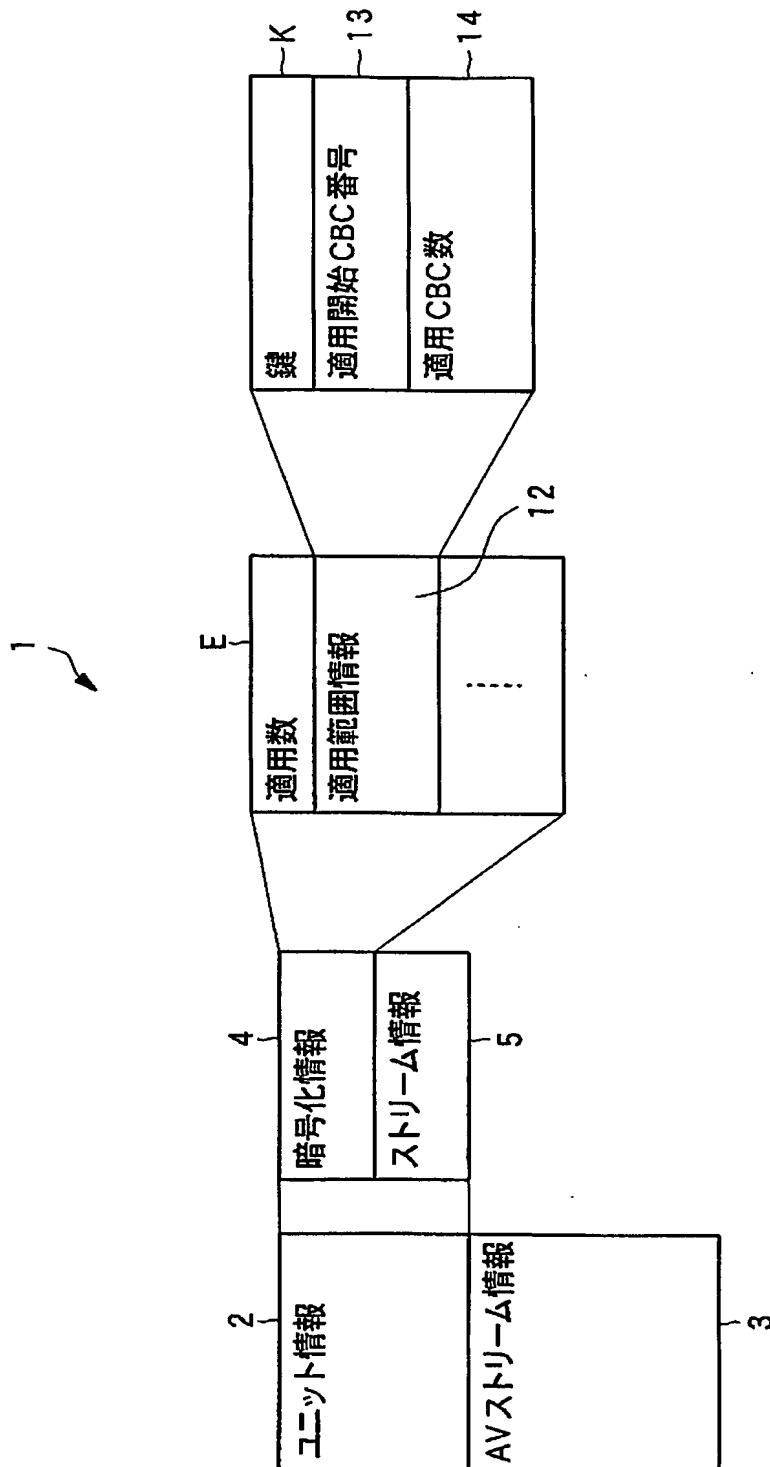
【0131】

- 1 HD
- 2 ユニット情報
- 3 AVストリーム情報
- 4 暗号化情報
- 5 ストリーム情報
- 8 ポインタテーブル
- 9 GOPサイズ
- 10 第1参照画像サイズ
- 11 鍵変更フラグ
- 12 適用範囲情報
- 13 適用開始CBC番号
- 14 適用CBC数
- 20 情報記録装置
- 21 デマルチプレクサ
- 22 映像、音声データデコーダ
- 24 レコードモジュール
- 25 CPU
- 26 メモリ
- 31 情報供給部
- 32 暗号化部
- 40 情報再生装置
- 41 情報出力部
- 42 非暗号化部
- 43 読出し部

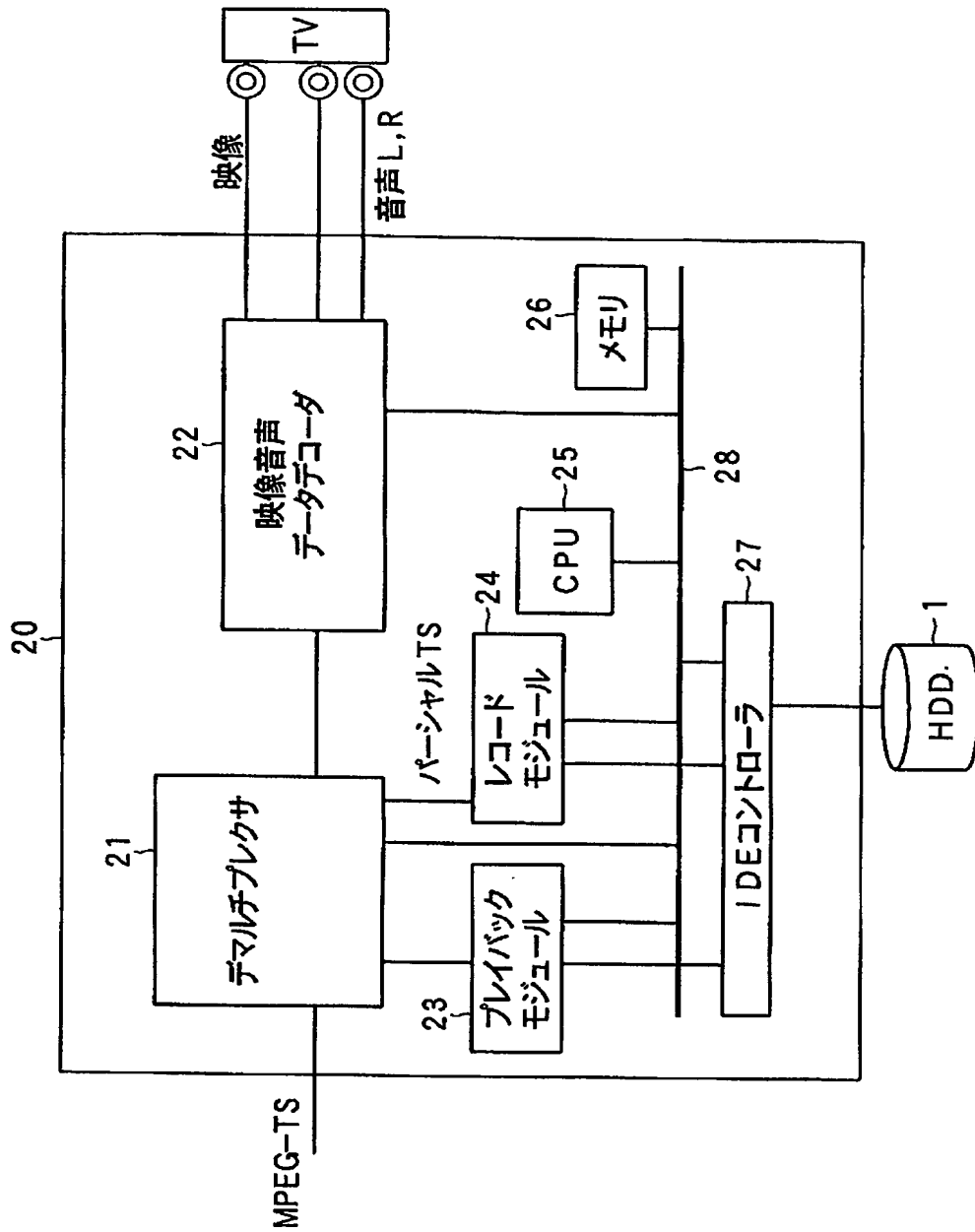
【書類名】 図面
【図 1】



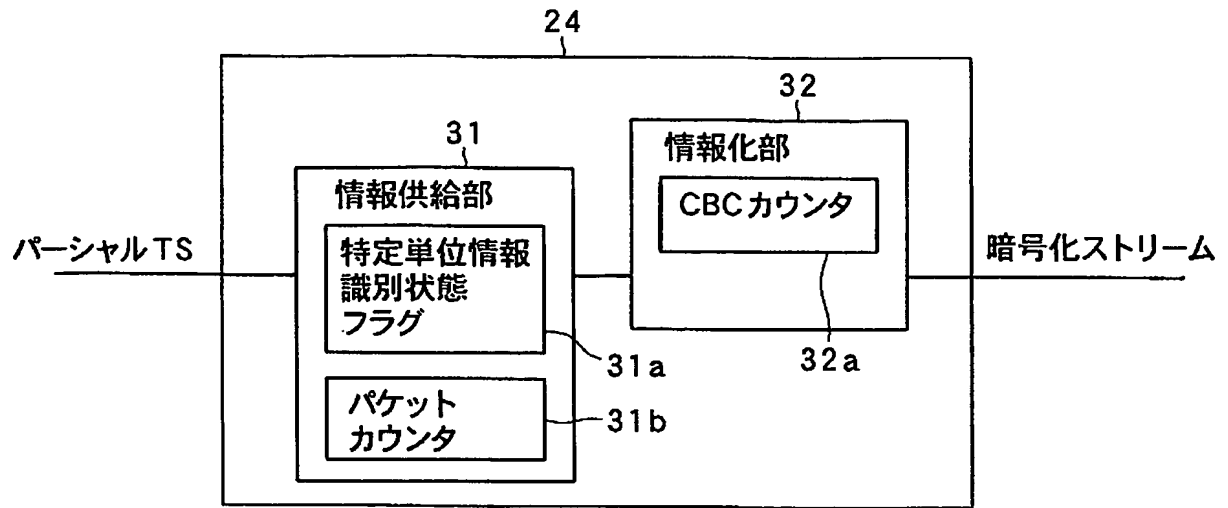
【図 2】



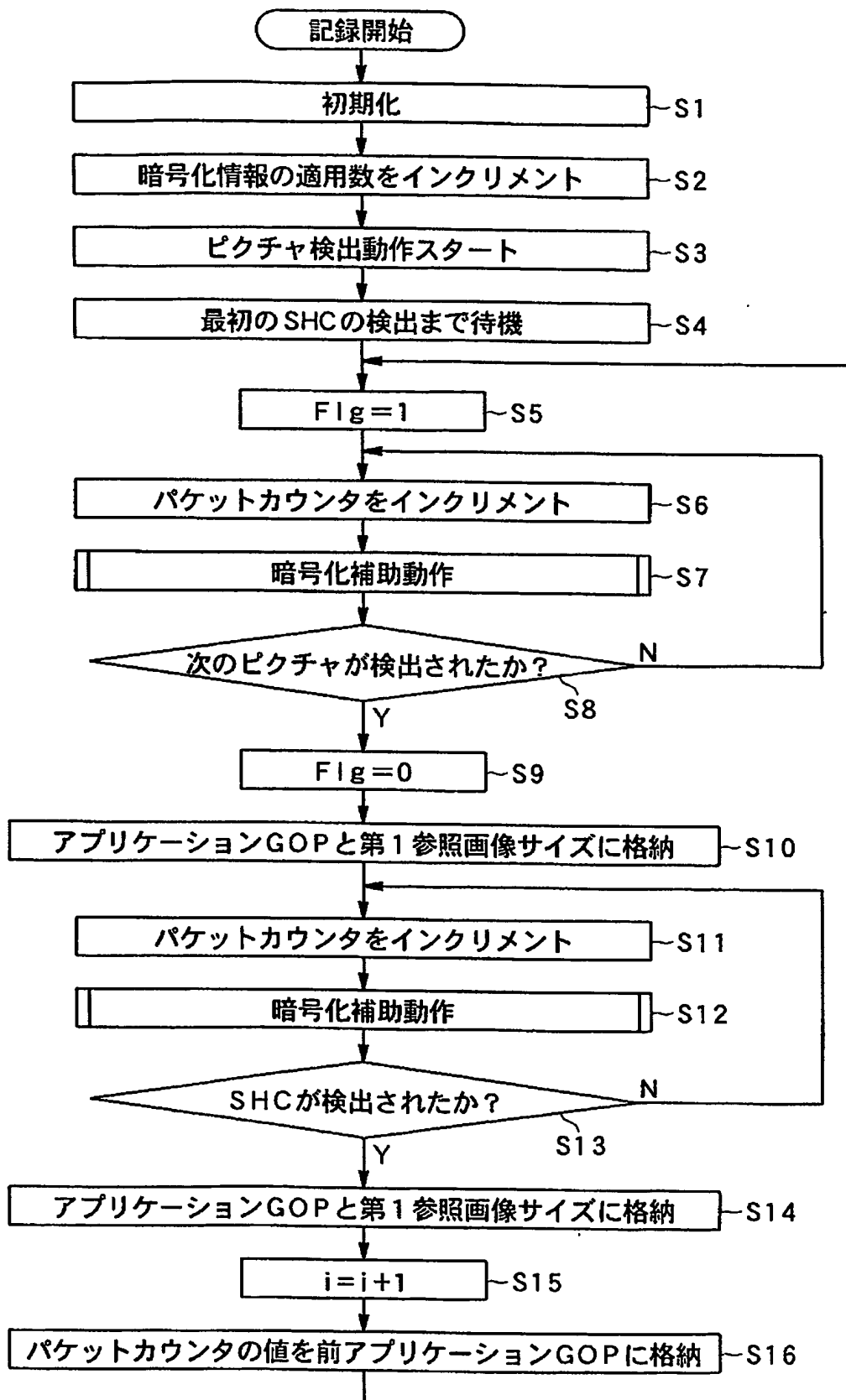
【図 3】



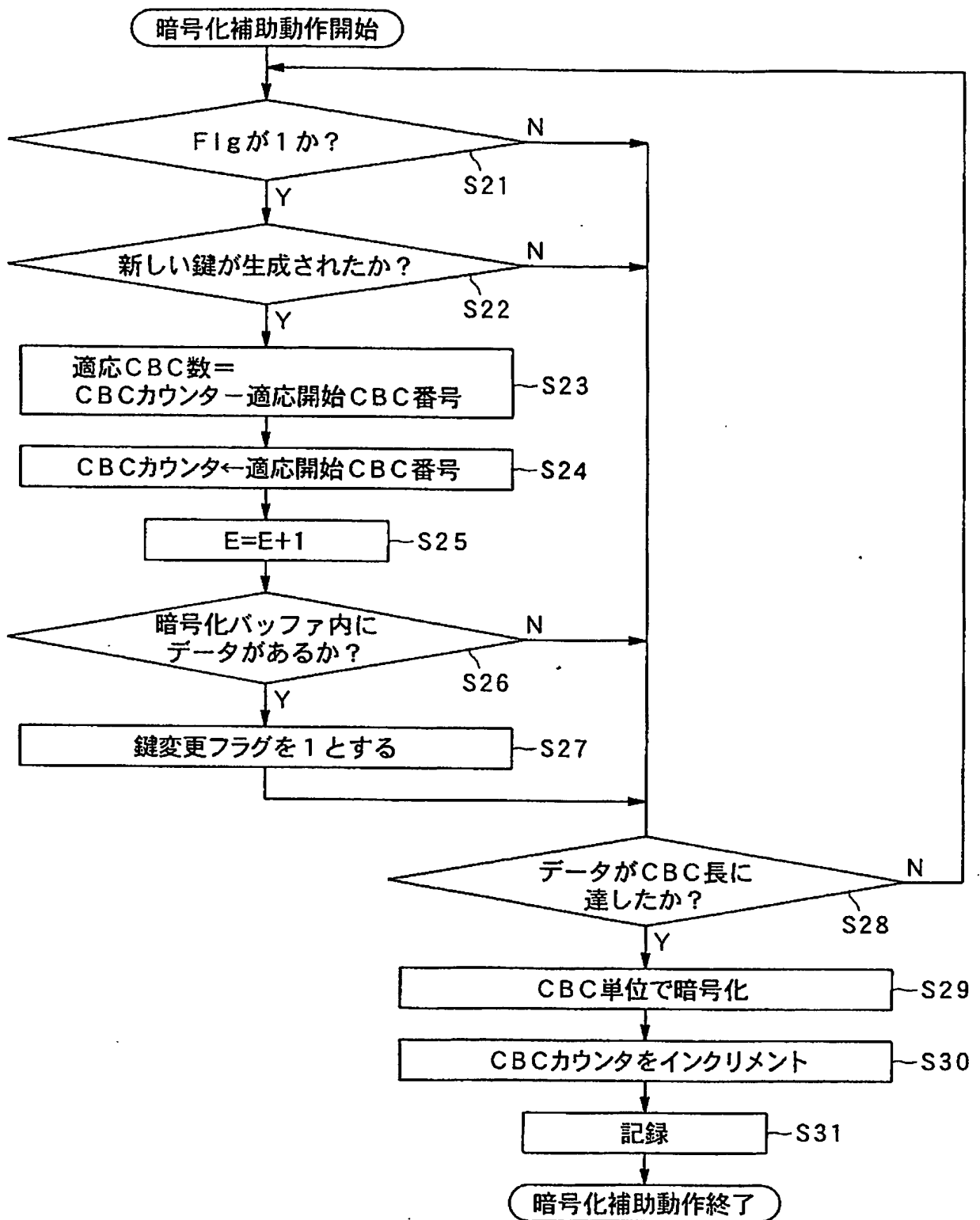
【図 4】



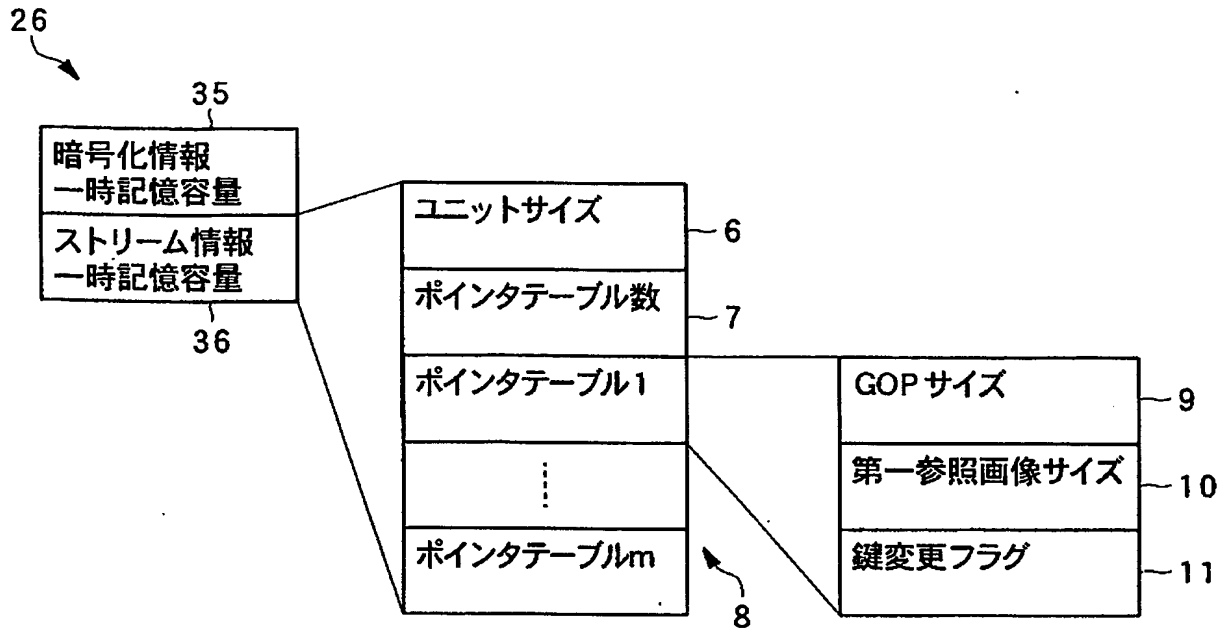
【図 5】



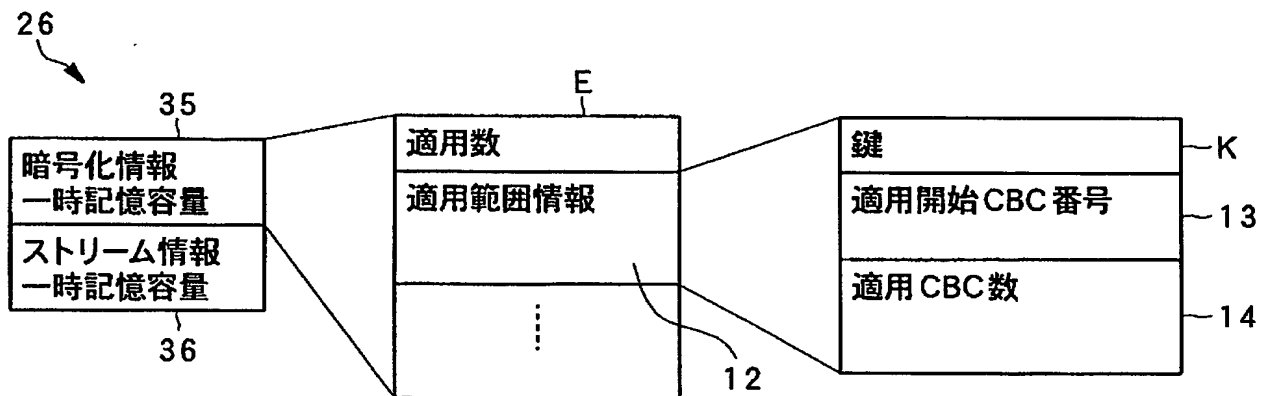
【図 6】



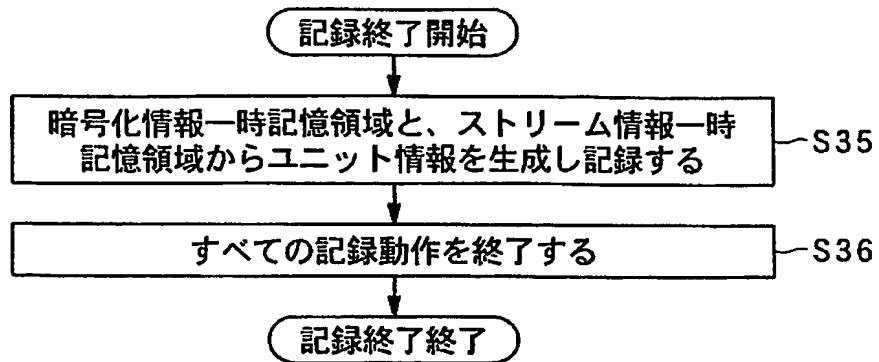
【図 7】



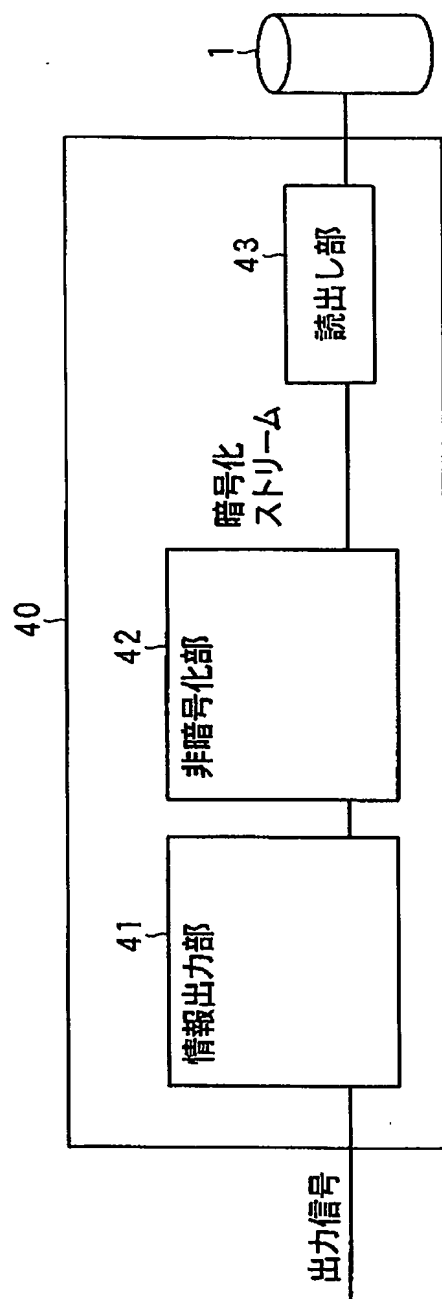
【図 8】



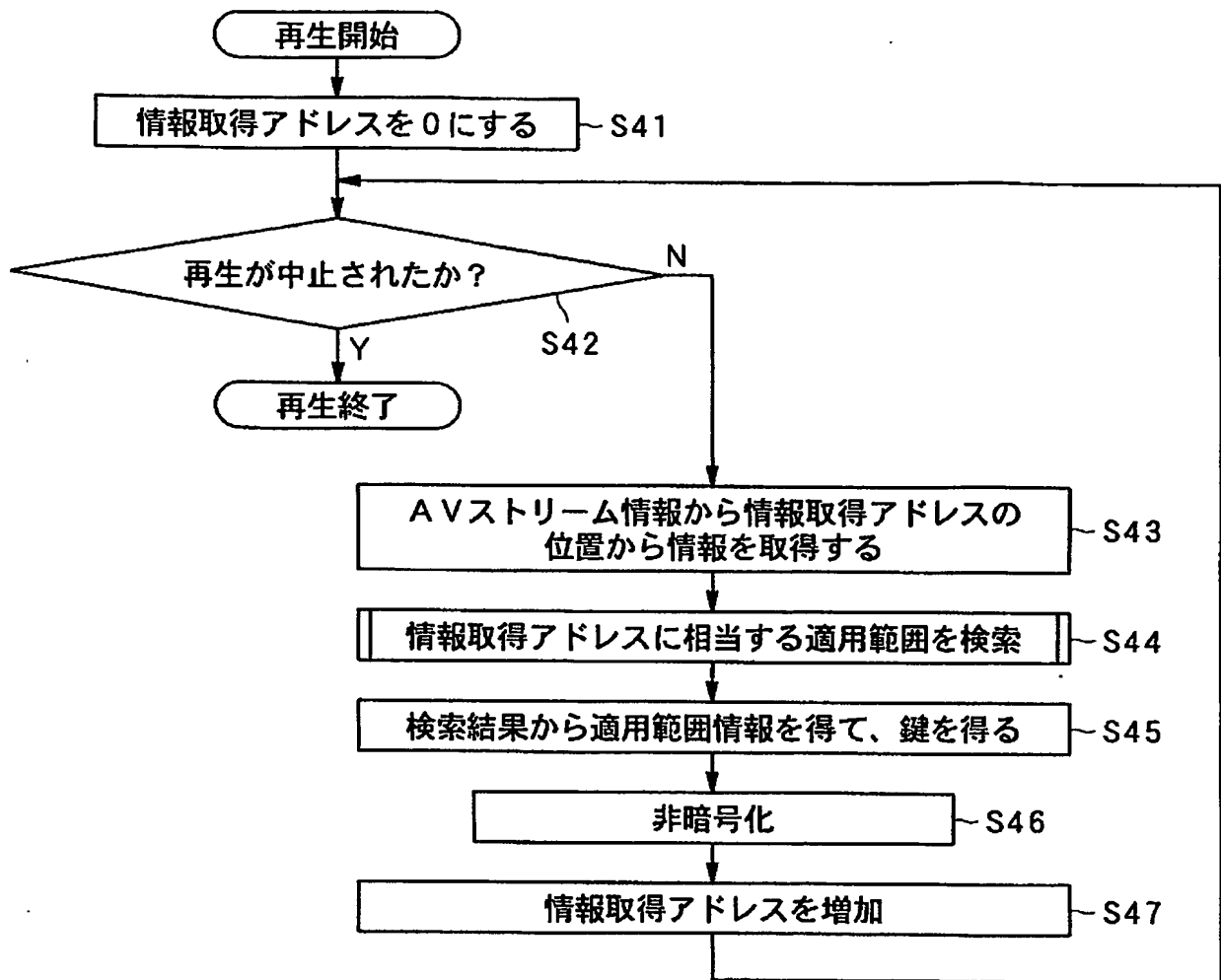
【図 9】



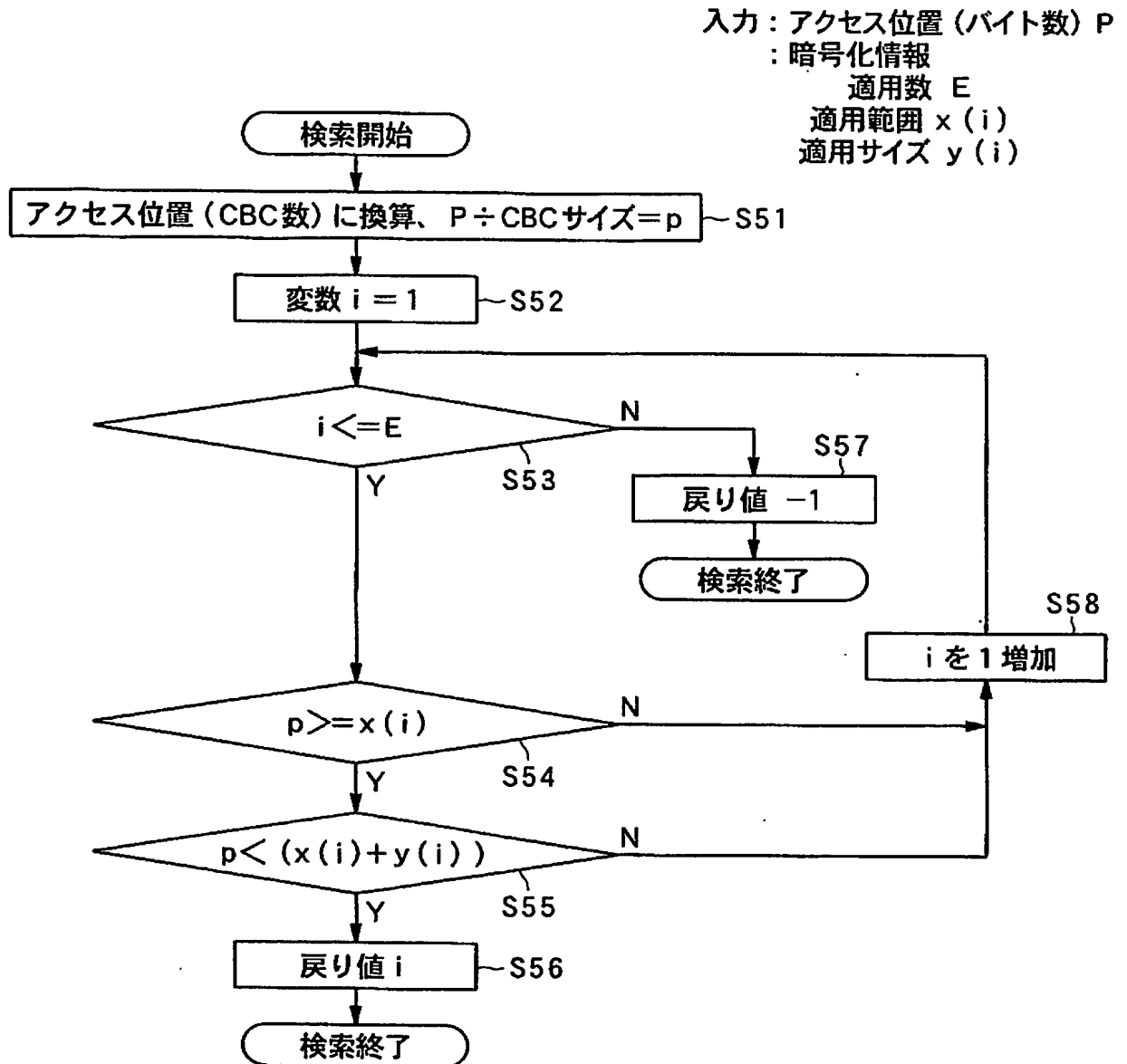
【図 10】



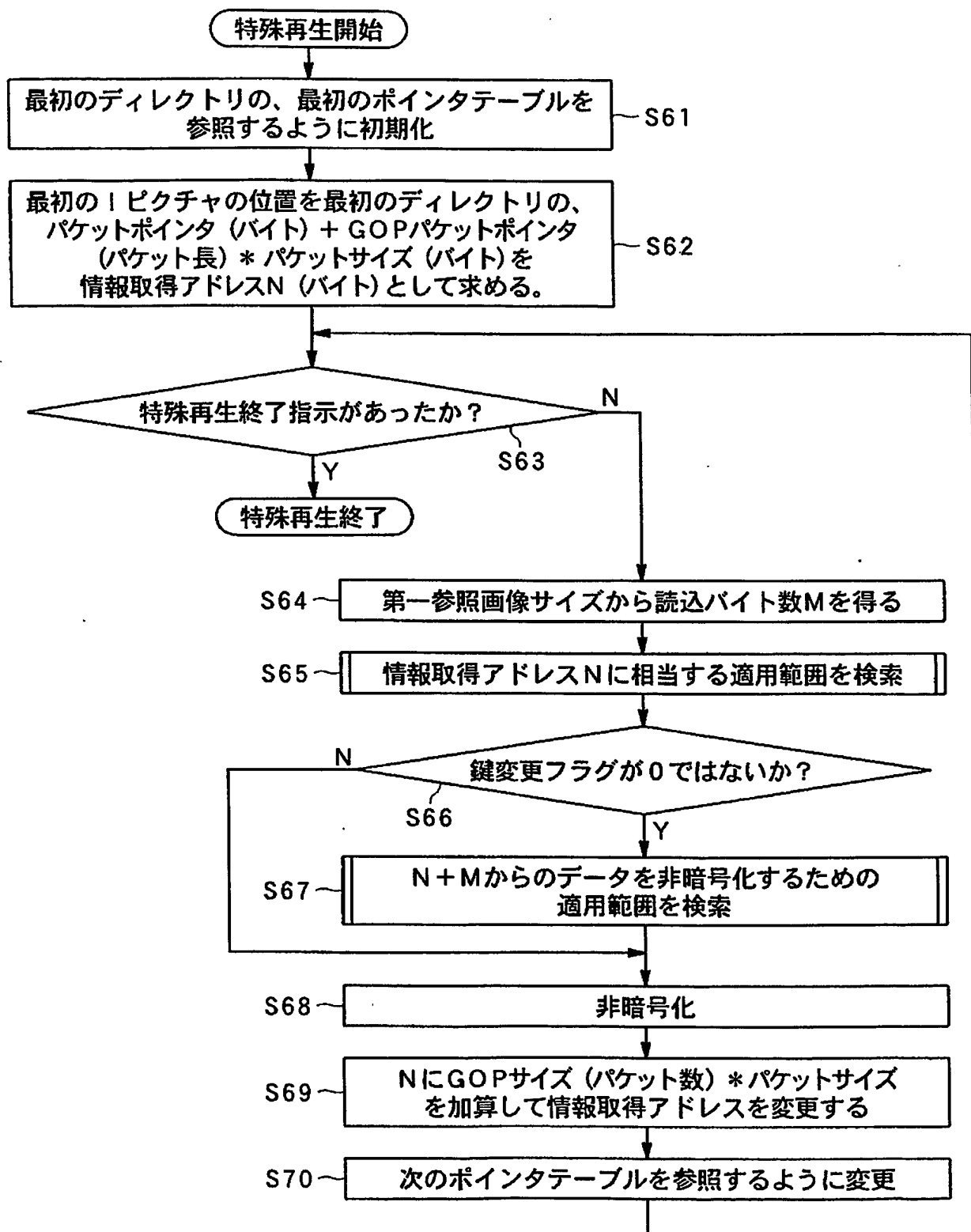
【図 11】



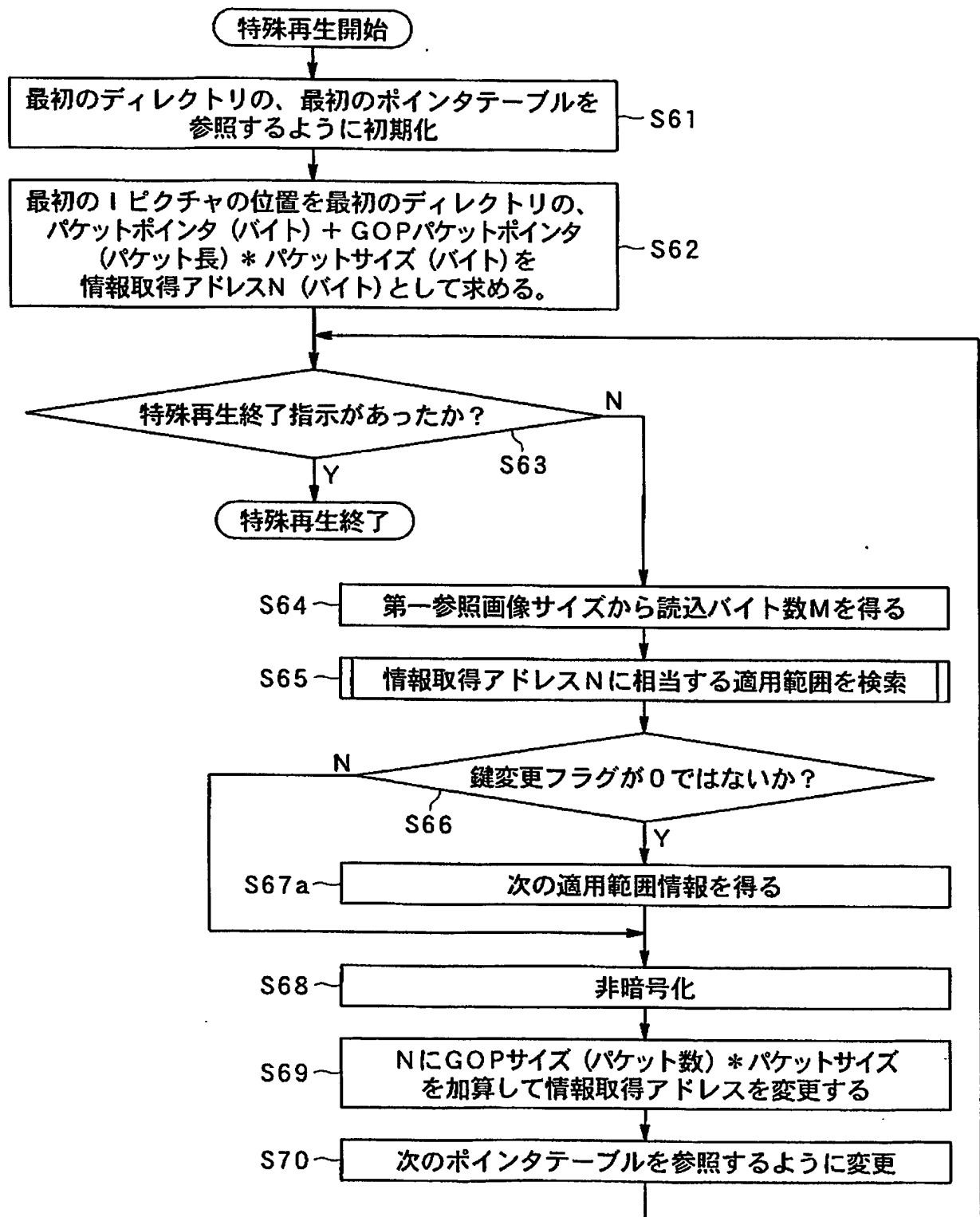
【図 12】



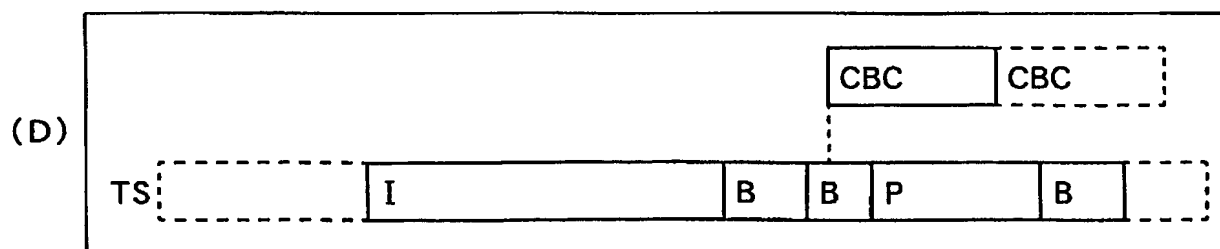
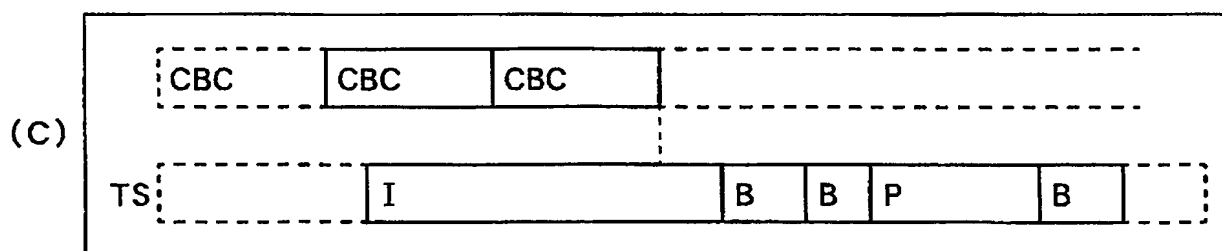
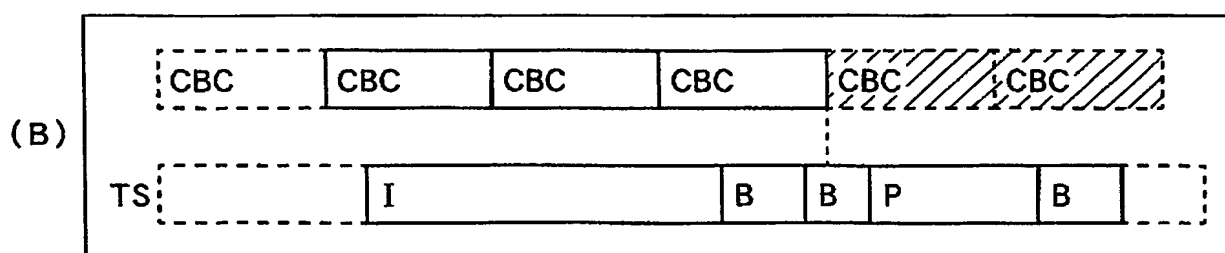
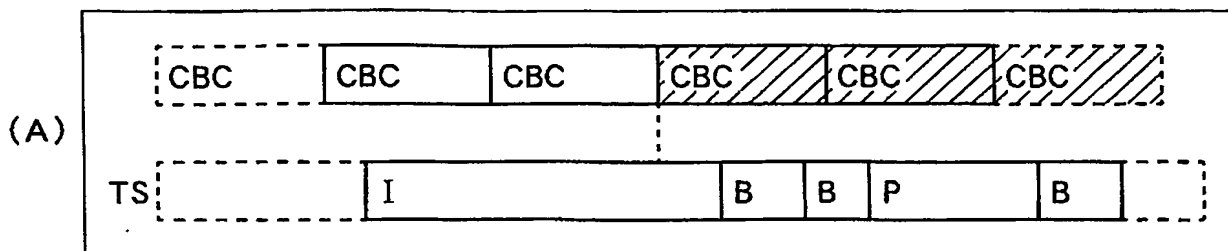
【図13】



【図 14】



【図 15】



【書類名】 要約書

【要約】

【課題】 暗号鍵の適用切り替わり時点を逐一算出する必要をなくし、円滑な処理を実行可能な情報記録媒体を提供すること。

【解決手段】 ハードディスク 1 には、アプリケーション GOP により構成される M P E G 2 規格におけるトランスポートストリームを、当該アプリケーション GOP と異なる C B C ブロックの境界において暗号鍵を変更しつつ暗号化して得られた暗号化情報が記録されている A V ストリーム情報 3 と、上記暗号化情報におけるアプリケーション GOP に含まれる I ピクチャの解読に複数の暗号鍵が必要か否かを示す鍵変更情報が記録されている鍵変更フラグ 1 1 と、が記録されている。

【選択図】 図 1

認定・付加情報

特許出願の番号	特願 2 0 0 3 - 3 7 3 0 9 7
受付番号	5 0 3 0 1 8 1 4 4 4 7
書類名	特許願
担当官	第八担当上席 0 0 9 7
作成日	平成 1 5 年 1 1 月 4 日

< 認定情報・付加情報 >

【提出日】 平成15年10月31日

特願 2003-373097

ページ: 1/E

出願人履歴情報

識別番号

[000005016]

1. 変更年月日
[変更理由]
住所
氏名

1990年 8月31日
新規登録
東京都目黒区目黒1丁目4番1号
パイオニア株式会社